Union Calendar No. 424

98TH CONGRESS *2d Session* | HOUSE OF REPRESENTATIVES | REPORT 98-738

IMPLEMENTATION OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

REPORT

together with

DISSENTING VIEWS

BY THE

PERMANENT SELECT COMMITTEE ON INTELLIGENCE

SECTION 108(b) OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, 92 STAT. 1783, 50 U.S.C 1808(b)

MAY 9, 1984.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

---

U.S. GOVERNMENT PRINTING OFFICE

31-006 O WASHINGTON : 1984

LETTER OF SUBMITTAL

HOUSE OF REPRESENTATIVES,
PERMANENT SELECT COMMITTEE ON INTELLIGENCE,
Washington, D.C., May 9, 1984.

Hon. THOMAS P. O'NEILL, Jr.,
Speaker of the House,
Washington, D.C.

DEAR MR. SPEAKER: On behalf of the Permanent Select Committee on Intelligence and pursuant to section 108(b) of the Foreign Intelligence Surveillance Act, 92 Stat. 1783, 50 U.S.C. 1808(b), I submit a report concerning the implementation of this Act. The Committee recommends that the Act should be permitted to continue in effect without amendment.

With every good wish, I am,
Sincerely yours,

EDWARD P. BOLAND, *Chairman.*

Enclosure.

Union Calendar No. 424

98TH CONGRESS, 2d Session | HOUSE OF REPRESENTATIVES | REPORT 98-738

IMPLEMENTATION OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

MAY 9, 1984.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. BOLAND, from the Permanent Select Committee on Intelligence, submitted the following

REPORT

together with

Dissenting Views

I. INTRODUCTION

The following report is submitted in fulfillment of the Committee's obligation under section 108(b) of the Foreign Intelligence Surveillance Act (FISA) which reads as follows:

> On or before each year after the effective date of this Act and on the same day each year for four years thereafter, the Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence shall report respectively to the House of Representatives and the Senate, concerning the implementation of this Act. Said reports shall include but not be limited to an analysis and recommendations concerning whether this Act should be (1) amended, (2) repealed, or (3) permitted to continue in effect without amendment.[1]

This is the fifth report filed by the Committee pursuant to section 108(b) and, therefore, the last which is required by statute. However, recognizing its special obligation to the House because of the secrecy which must envelop foreign intelligence electronic sur-

[1] 92 Stat. 1783, 50 U.S.C. 1808(b).

31-006 O

veillance, the Committee will continue to issue an unclassified annual report on the implementation of FISA.

II. IMPLEMENTATION

The foreign Intelligence Surveillance Act was signed into law by President Carter on October 25, 1978, and became fully effective August 16, 1979.[2]

The first complement of judges of the Foregin Intelligence Surveillance Court (FISC) and the Foreign Intelligence Court of Review was designated by the Chief Justice on May 16, 1979.[3]

The applicants for electronic surveillances under FISA are in almost all cases the National Security Agency or the Federal Bureau of Investigation. Targets of NSA surveillance are approved by a committee consisting of representatives of the National Security Council, the Director of Central Intelligence and the Secretaries of State and Defense. The Attorney General is notified of the Committee's approval. If FBI operational support is required, the NSA requests it of the FBI Director in writing. Typically the actual court application is prepared in the General Counsel's Office at NSA using a format previously approved by the Office of Intelligence Policy and Review (OIPR) of the Department of Justice. If the application involves an unusual target or technique, the drafting will be coordinated with OIPR. When the application is ready, it is presented to the Secretary of Defense for his review and certification that the information sought is foreign intelligence and otherwise satisfies the statutory certification requirements.[3a] Once he has made the certification, the application is forwarded to OIPR. After OIPR review, it is presented to the Attorney General for approval of its submission to the Court.

FBI field offices initiate FBI requests for surveillances. These are reviewed at FBI Headquarters and a memorandum is prepared from an Assistant Director to the Department of Justice setting forth the basis for the surveillance and requesting that an application be prepared. Attorneys at OIPR review the memorandum to determine whether it meets the statutory standard, with particular attention to the probable cause requirements. They then prepare a draft application which is returned to the FBI for review by intelligence personnel and FBI attorneys. Once it has been signed by the applicant agent and certified by the FBI Director, it is returned to OIPR for final review. It is then sent to the Attorney General for his approval of its submission to the Court.

On regularly scheduled Court days applications approved by the Attorney General are delivered to the Clerk of the FISA Court, with copies for the Court and the Court's legal adviser. They review the application in chambers. When the Court convenes, the applicant and the OIPR attorney who prepared the application appear before the Court, answer any questions the Court may pose, and swear to the accuracy of the application. If the Court is satisfied, it issues the order or orders prepared by the Executive Branch which are appended to the application. The primary order consists

[2] See Section 301 of the Act, 50 U.S.C. 1801 note.
[3] See Appendix A for the list of judges as of May 1, 1984.
[3a] See Section 104 of the Act.

of the authorization for the applicant agency to conduct the surveillance. There may, however, be secondary orders directed to communications common carriers, landlords or others, instructing them to render necessary assistance to the government. After the Clerk has recorded the orders and affixed the seal of the Court, the orders are returned to the applicant agency for execution.

While the judges of the Court have been designated from seven different judicial circuits, the Court always sits in Washington, D.C. Normally a judge is scheduled to sit one or two days, twice a month, on a rotational basis. Applications requiring action in between scheduled Court days, usually those that arise unexpectedly, are presented to one of two local judges who are members of the Court. The bulk of the applications are pesented on regularly scheduled court days.

III. OVERSIGHT

In the approximately 5 years since the new statutory procedures for foreign intelligence electronic surveillance within the United States have been in effect, the Committee has received 10 written reports on its implementation from the Attorney General.

It is through these written reports, which are classified, and through regular discussions with the relevant executive branch personnel, that the Committee has been able to obtain the information necessary to perform effectively its oversight function in this sensitive area.

Congressional oversight is particularly important in regard to electronic surveillance performed under the Foreign Intelligence Surveillance Act. In enacting FISA, the Congress concluded that the necessary secrecy with which foreign intelligence activities must be conducted justified establishing procedures for foreign intelligence electronic surveillance that differ from those which regulate electronic surveillance for law enforcement purposes.

These differences (see Appendix B) place a unique and heavy burden on the two Intelligence Committees of the Congress to ensure that the FISA is being interpreted and applied as intended, that what was intended remains wise policy, and that probable cause determinations are correct and consistent. This burden lies with the Intelligence Committees because, unlike what obtains in connection with law enforcement searches, the bench, the bar, the press, and the public are not permitted, after the fact, to review or comment on the decisions of the Foreign Intelligence Surveillance Court.

The Committee has a duty to the Congress and the public to be especially vigilant and thorough in its oversight of surveillances of U.S. persons. Immediately prior to the enactment of FISA, there existed, according to the testimony of Attorney General Bell, two ongoing cases of electronic surveillance of U.S. persons in the United States for foreign intelligence purposes. This number has increased each year since the enactment of FISA.[4]

[4] The overwhelming number of FISA surveillances continue to be direted against non-U.S. person targets.

In the past, Members of the Committee have reviewed the full text of a small number of U.S. person FISA Court order applications and the Committee staff has reviewed a small number of redacted applications. In some instances, the redactions in the applications reviewed by staff have been so extensive as to reduce significantly the utility of the review process.

Therefore, as noted above, the Committee has based its oversight judgments largely on its review of the Attorney General's semiannual classified reports and on extensive discussion with officials of the Department of Justice, Office of Intelligence Policy and Review, the FBI, and the NSA, in whom the Committee continues to place its trust and confidence.

However, effective oversight must be based on a more permanent foundation than good working relationships. Members of Congress and their staffs, and exectuive branch officials and their staffs, come and go. Soon, few will remain who were present at the creation of FISA.

With the foregoing in mind, and with the continuing increase in the use of the authority provided by FISA to electronically surveil U.S. persons, and others, the Committee has concluded that its continued ability to state with confidence, as it has in the past, that U.S. person surveillances are being conducted fully within the letter and spirit of the law, must depend on a more thorough review of applications. This will include a regular schedule of review of a larger number unredacted applications by both Members and a limited number of staff selected by the Committee. The Committee expects the Department of Justice to cooperate in this effort.

IV. STATISTICAL SUMMARY

Section 107 of the Foreign Intelligence Surveillance Act provides that:

> In April of each year, the Attorney General shall transmit to the Administrative Office of the United States Courts and to Congress a report setting with respect to the preceding calendar year—
>
> (a) the total number of applications made for orders and extensions of orders approving electronic surveillance under this title; and
>
> (b) the total number of such orders and extensions either granted, modified, or denied.

On April 4, 1983, the Attorney General submitted the report required by section 107. The pertinent section of the report stated:

> During calendar year 1982, 473 applications were made for orders and extensions of orders approving electronic surveillance under the Act. The United States Foreign Intelligence Surveillance Court issued 475 orders granting authority to the Government for the requested electronic surveillances. No orders were entered which modified or denied the requested authority.[5]

[5] The number of orders exceeds the number of applications for either of two reasons. A single application may request authority to surveil more than one facility of the same foreign power.

Continued

On March 6, 1984, the Attorney General submitted the report for calendar year 1983. It notes 549 applications for orders and extension of orders, 549 orders issued by the court, and no modifications or denials.

There has been a continuing increase in the number of FISA surveillances since 1980, the first full year of FISA operation (see Appendix C). While the Committee, for security reasons, cannot discuss the categories of surveillances with any specificity, it can be noted that the significant increases in the number of surveillances occur in the categories of foreign power and non-U.S. person agent of foreign power surveillances, rather than in the U.S. person category, although there has been an increase in the latter.

In addition, because surveillances of agents of foreign powers must be renewed every 90 days, the calendar year number of application figures may be misleading. For example, if the same agent of a foreign power is continuously targeted for one year, there will be at least three, and possibly four, applications for that year.

V. NATIONAL SECURITY AGENCY "WATCHLIST"

The first definition of electronic surveillance in FISA (section 101(f)(1)) affects the use of NSA computer seletion technology to retrieve the international communications of a United States person when that person is in the United States and NSA intentionally targets that person. Targeting is accomplished by using a person's name, or other unique identifier, to select that person's communications. This definition was specifically added to the Act to regulate an NSA program of the late sixties and early seventies which was commonly referred to as "watchlisting."

NAS fully understands and abides by this provision. However, a civil suit, *Jabara* v. *Webster,* 691 F.2d272 (6th Cir. 1982), in which the plaintiff alleged that watchlisting occurred, appears to have caused some confusion outside NSA as to the applicability of this definition to NSA's monitoring of international communications. NSA understands this definition to require a court order before it searches through communications as they are collected for communications of a particular United States person when that person is in the United States. This requirement applies to searches of previously collected communications while those communications reside in data bases of unprocessed intercept. Once a communication is retrieved from such a data base and is used to develop an intelligence report, the FISA no longer applies to the subsequent retrieval of that intelligence report. It is NSA's practice to delete a United States person's name from intelligence report; and as a practical matter, it is not possible to retrieve NSA intelligence reports issued since 1975 by the names of United States persons.

If the circumstances of the *Jabara* case occurred today, NSA could seek an order from the Foreign Intelligence Surveillance Court to select any international communications that the target would send or receive after the request. If necessary, and after obtaining a court order, the NSA could review available, unprocessed

In such circumstances, more than one order results from one application. A single application may also request authority to surveil one facility of a foreign power, by the use of different surveillance techniques.

intercept. Finally, the NAS could review its intelligence reports to determine if any of the concerned the target; this review would not require a court order.

VI. LITIGATION

Since the Committee's last report, the legality of FISA surveillances has been upheld by a federal district court in three cases: *United States* v. *Kozibioukian,* CR. 82-460 (C.D. Cal.); *United States* v. *Hovsepian,* CR. 82-917 (C.D. Cal.); and *United States* v. *Harper,* CR. 83-0770 (N.D. Cal). Two other cases are pending in which FISA is an issue: *United States* v. *Kostadinov,* CR. 83-616 (S.D. N.Y.); and *United States* v. *Zehe,* CR. 83-296 (D. Mass.).

There have been six instances since the inception of FISA in which the target of a FISA surveillance has been prosecuted. Set out at Appendix D is a statement of the Department of Justice's position (contained in a letter from Assistant Attorney General McConnell to Representative Robert Kastenmeier, Chairman, Subcommittee on Courts, Civil Liberties, and the Administration of Justice, House Committee on the Judiciary) that a FISA surveillance (in contrast to a law enforcement electronic surveillance under Title III of the Omnibus Crime Control and Safe Streets Act) may be employed, even when prosecution is contemplated, as long as significant foreign intelligence information is sought.

While expressing no opinion at this time as to the legal correctness of the Department's decision, the Committee is of the view that, even if the Department's position is arguably supported by the relevant legislative history, the wiser course is to utilize Title III, rather than FISA, once prosecution is contemplated, unless articulable reasons of national security dictate otherwise.

VII. MINIMIZATION

Central to the FISA scheme of authorizing electronic surveillance within the United States for foreign intelligence purposes, while assuring full protection for the privacy interests of U.S. persons, is the "minimization" process.[6]

The minimization procedures mandated by FISA provide vital safeguards because they regulate the acquisition, retention, and dissemination of information about U.S. persons, including persons who are not the authorized targets of surveillance. Section 101(h) of FISA defines "minimization procedure" as:

> (1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

[6] See Appendix E and Appendix F for the NSA and FBI minimization procedures. The procedures provided in the Appendices have been subjected to security deletions which make no substantive difference.

(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1), shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or access its importance;

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and

(4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 102(a), procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than twenty-four hours unless a court order under section 105 is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

Because these procedures are such a significant element in the production afforded by FISA, effective oversight of the minimization process is crucial.[7]

The primary responsibility for conducting such oversight rests with those agencies conducting surveillances (the NSA and the FBI) and with the Department of Justice.

Policies and procedures in effect at NSA require that all persons handling materials subject to FISA minimization procedures be properly trained in those procedures. Minimization procedures are taught in NSA training courses and stressed in on-the-job training. Individual responsibility of NSA employees for compliance with the procedures is set forth in appropriate NSA regulations and reinforced by periodic reminders issued by the Office of Personnel. Employees responsible for implementing procedures unique to FISA operations are provided special training tailored to those procedures prior to being granted access to the collected materials. The training is conducted in part by the Office of General Counsel, which also provides guidance and assistance in implementing FISA operations. The Inspector General's Office conducts periodic inspections of those NSA elements which conduct FISA operations. The inspection focuses on awareness of and compliance with minimization procedures.

NSA's collection activities are directed at information concerning the capabilities, intentions, and activities of foreign governments. Therefore, in many cases, incidentally acquired information about U.S. persons has no relevance to NSA's mission. When information is relevant to foreign intelligence collection, NSA's procedures are very restrictive. As a practical matter, they can be applied and ob-

[7] See generally, H. Schwartz, "Oversight of Minimization Compliance Under the Foreign Intelligence Surveillance Act: How the Watchdogs Are Doing Their Jobs", 12 Rutgers L.J. 405 (1981).

served without difficulty because there is less likelihood that foreign intelligence information that needs to be disseminated to analysts and policymakers will contain information concerning U.S. persons.

Dissemination of information concerning United States persons is strictly controlled and receives close scrutiny. When information concerning United States persons is disseminated, it is usually done without providing the person's identity. Government agencies may request a deleted identity but must provide an explanation of need for that identity. These requests are reviewed by several organizational echelons, including the NSA Office of General Counsel, to assure that, in light of the explanation, NSA may release the identity consistent with the criteria in the minimization procedures. Such releases must be approved by the Deputy Director for Operations, or if the dissemination is for law enforcement purposes, by the Director of NSA.

The FBI is the domestic counterintelligence arm of the U.S. intelligence community. Thus, unlike NSA, its FISA targets often involve U.S. persons and its minimization procedures are accordingly geared to this greater degree of involvement with U.S. persons.

Minimization in regard to FBI conducted surveillance begins at the earliest step of the interception process by the individuals who actually listen to the surveillance contemporaneously or listen to tapes of automatically acquired information. These individuals are called surveillance monitors.

The monitors enter into a surveillance log book summaries of those conversations that, in the opinion of the monitor, contain relevant foreign intelligence information. Information that is not logged is not retrievable at a later time. Information that is logged must be both "foreign intelligence information" as defined in the FISA, and relevant to the purpose of the surveillance. Monitors receive extensive training, both at FBI Headquarters and in the field, on the minimization process. In addition, they are in constant contact with the FBI Special Agent assigned to each surveillance. Each Agent receives detailed instruction on the minimization process and undergoes periodic in-service training. The case Agents are thus in a position to advise the monitors both as to what is or is not foreign intelligence information and on what foreign intelligence information should be logged.

The surveillance logs are regularly forwarded to the case Agent or to FBI Headquarters, depending on the circumstances. It is at such a supervisory level that minimization of retention and dissemination, as set out in the procedures, is conducted.

The Office of Intelligence Policy and Review (OIPR) of the Department of Justice oversees the minimization process engaged in by the NSA and the FBI.

The NSA minimization procedures focus primarily on retention and dissemination of information identifying U.S. persons. NSA retains records of information disseminated and periodically (and in all cases, at least once a year) attorneys from OIPR visit NSA to review these records on a random selection basis. In unusual cases, NSA attorneys consult with OIPR prior to a proposed dissemination where there is a question of compliance with the minimization procedures.

OIPR oversees the FBI's minimization process in a similar fashion. OIPR attorneys visit the major FBI field offices and conduct a detailed review of the surveillance logs. They also talk with the surveillance monitors and supervisory personnel to determine whether they understand the requirements or have identified particular problems or questions.

Should a violation of the minimization procedures occur by either NSA or FBI, a complete report is made to the FISA Court, the Attorney General, the President's Intelligence Oversight Board, and the Senate and House Intelligence Committees.

The Foreign Intelligence Surveillance Court also has a vital role to play in the oversight of minimization. In addition to deciding in each case whether the minimization procedures attached to the application meet the definition of minimization procedures contained in FISA, the judge "may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, or disseminated." (Section 105(d)(3) of FISA). This provision contemplates periodic examination by FISA judges of surveillance logs, intelligence disseminations, or other material relevant to an assessment of compliance with the minimization procedures.

The Senate and House Intelligence Committees, of course, also oversee the minimization process. As with the other provisions of the Act, this Committee has relied on the classified Attorney General reports and on extensive discussions with NSA, FBI, and OIPR personnel to discharge its responsibilities in this area. Such discussions have included staff communications with FBI surveillance monitors.

VIII. RECOMMENDATIONS

In 1976, Attorney General Edward H. Levi, while testifying before the Senate Select Committee on Intelligence on the proposed Foreign Intelligence Surveillance Act, stated:

> Enactment of the bill will, I believe, provide major assurance to the public that electronic surveillance will be used in the United States for foreign intelligence purposes pursuant to carefully drawn legislative standards and procedures. The bill insures accountability for official action. It compels the Executive to scrutinize such action at regular intervals. And it requires independent review at a critical point by a detached and neutral magistrate.
>
> In providing statutory standards and procedures to govern the use of electronic surveillance for foreign intelligence purposes in this country and in establishing critical safeguards to protect individual rights, the bill also insures that the President will be able to obtain information essential to protection of the Nation against foreign threats. While guarding against abuses in the future, it succeeds, I trust, in avoiding the kind of over reaction against abuses of the past that focuses solely on these abuses, but is care-

> less of other compelling interests. To go in that direction would bring a new instability and peril.[8]

In 1978, Attorney General Griffin B. Bell testifying on the same subject before this Committee, stated:

> If enacted, the bill would stand as a significant monument to our national commitment to democratic control of intelligence functions . . .
>
> As President Carter noted when he announced this bill, "one of the most difficult tasks in a free society like our own is the correlation between adequate intelligence to guarantee our nation's security on the one hand, and the preservation of basic human rights on the other." It is a very delicate balance to strike, but one which is necessary in our society. In my view this bill strikes the proper balance. It sacrifices neither our national security nor our civil liberties, and assures that the dedicated and patriotic men and women who serve this country in intelligence positions will have the affirmation of Congress that their activities are proper and necessary.[9]

We have now had five years in which to observe in operation the legislation these two distinguished Attorneys General worked so hard to enact and about which they spoke so eloquently.

The Committee is of the opionion that FISA did, in fact, strike a proper balance between the security of the Nation and the individual rights of its people, that FISA surveillances are being utilized only to collect legitimate foreign intelligence information, that such surveillances are being conducted well within the letter and spirit of the Act, and that adherence to the substantive and procedural safeguards contained in FISA has not adversely affected the national intelligence mission.

The Committee recommends that the Act be permitted to continue in effect without amendment.

---

[8] *Electronic Surveillance Within the United States for Foreign Intelligence Purposes,* Hearings before the Subcommittee on Intelligence and the Rights of Americans of the Select Committee on Intelligence, United States Senate, 94th Congress, 2nd Session (1976), Page 76.

[9] *Foreign Intelligence Electronic Surveillance,* Hearings before the Subcommittee on Legislation of the Permanent Select Committee on Intelligence, House of Representatives, 95th Congress, 2nd Session (1978), Page 7.

APPENDIX A

Judges Designated by the Chief Justice of the United States Pursuant to Section 103 of the Foreign Intelligence Surveillance Act of 1978 (as of May 1, 1984).

FOREIGN INTELLIGENCE SURVEILLANCE COURT

John Lewis Smith, Jr., (presiding judge), U.S. District Court, District of Columbia.

Albert V. Bryan, Jr., U.S. District Court, Eastern District of Virginia.

Frederick B. Lacey, U.S. District Court, District of New Jersey.

William C. O'Kelley, U.S. District Court, Northern District of Georgia.

Frederic A. Daugherty, U.S. District Courts, Northern, Eastern, and Western Districts of Oklahoma.

Dudley B. Bonsal, U.S. District Court, Southern District of New York.

James E. Noland, U.S. District Court, Southern District of Indiana.

FOREIGN INTELLIGENCE SURVEILLANCE COURT REVIEW

A. Leon Higginbotham, Jr., (presiding judge), U.S. Court of Appeals for the Third Circuit.

James E. Barrett, U.S. Court of Appeals for the Tenth Circuit.

John A. Field, Jr., U.S. Court of Appeals for the Fourth Circuit.

APPENDIX B

COMPARISON WITH TITLE III WARRANTS

Although FISA is patterned after Title III of the Omnibus Crime Control and Safe Streets Act of 1968, which authorizes and regulates electronic surveillance for law enforcement purposes, there are the following significant differences, among others:

Title III requires a finding of probable cause that the target "is committing, has committed, or is about to commit" one of the enumerated offenses. FISA, for most U.S. person targets, requires a finding of probable cause that certain intelligence activities, which "may involve" a criminal violation, are being conducted on behalf of a foreign power.

Title III warrants must be renewed every 30 days. FISA permits suveillances of individuals for up to 90 days and of some foreign powers for up to one year.

Title III requires that notice of the surveillance be given to the target not more than 90 days after the termination of the surveillance. FISA requires notice to the target only if evidence obtained or derived from the surveillance is to be used in a criminal prosecution of the target.

Title III warrants are issued by whichever of the 515 federal district court judges has territorial jurisdiction over the site of the surveillance. FISA warrants are issued by one of the seven federal judges sitting on the FISC, each of whom has nationwide jurisdiction.

APPENDIX C

Number of FISA court orders

Calendar year:	*Orders*
1979	199
1980	319
1981	431
1982	475
1983	549

APPENDIX D

U.S. DEPARTMENT OF JUSTICE,
OFFICE OF LEGISLATIVE AFFAIRS,
Washington, D.C., September 26, 1983.

Hon. ROBERT W. KASTENMEIER,
Chairman, Subcommittee on Courts, Civil Liberties and the Administration of Justice, Committee on the Judiciary, House of Representatives, Washington, D.C.

DEAR MR. CHAIRMAN: In response to the questions attached to your letter of August 17, 1983, concerning the Foreign Intelligence Surveillance Act, we are forwarding the attached answers.

Please let us know if we can be of any further assistance regarding this matter.

Sincerely,

ROBERT A. MCCONNELL,
Assistant Attorney General.

Attachment.

3. It is our view that the logic of *United States* v. *Truong,* 629 F.2d 908 (4th Cir. 1980) has little vitality after the enactment of the Foreign Intelligence Surveillance Act. In *Truong* the Court held a warrantless foreign intelligence electronic surveillance was lawful only when the purpose of the surveillance was "primarily" for foreign intelligence purposes. In so holding the court recognized that, in view of the warrantless nature of pre-FISA foreign intelligence electronic surveillances, there was no opportunity for an impartial magistrate to review the probable cause for a surveillance until after the surveillance had been implemented and a party who has been overheard challenged the legality of the surveillance in litigation. Under FISA the probable cause for a surveillance is reviewed by a Federal District Court judge prior to implementation, at which time the purpose of the surveillance is also reviewed—thus, the *Truong* rationale would no longer apply.

Since the enactment of FISA, the two courts which have addressed the issue of whether the *Truong* primary purpose test still applies in the context of a FISA surveillance appear to have reached somewhat different conclusions. In *United States* v. *Falvey,* 540 F. Supp. 1306 (E.D.N.Y. 1982), Judge McLaughlin held that the *Truong* primary purpose test no longer applied, since a FISA surveillance is authorized by court order.

> What the defendants steadfastly ignore, however, is that in this case—unlike *Truong*—a court order was obtained authorizing the surveillance. After the surveillance was conducted in *Truong* (without a warrant), Congress enacted FISA, imposing a warrant requirement to obtain foreign intelligence information. *See* pp. 1312–1313, *supra.* An

> order authorizing the surveillance in this case was lawfully obtained pursuant to FISA. *See* p. 1316. Accordingly, all the relevant evidence derived therefrom will be admissible at trial. [Footnote omitted.]

540 F. Supp. at 1314. In *United States* v. *Megahey,* 553 F. Supp. 1180 (E.D.N.Y. 1982), on the other hand, Judge Sifton implied (but did not specifically hold) that the *Truong* test for warrantless foreign intelligence surveillance still applies to surveillances under FISA. 553 F. Supp. at 1189. While we believe that the *Falvey* decision on the inapplicability of the *Truong* primary purpose test to FISA surveillances is the correct one, we have invited the district courts, which subsequent to the *Megahey* decision, were considering the legality of FISA surveillances, to make the same analysis of the FISA surveillance as was done by Judge Sifton in *Megahey.*

Accordingly, it is our view that even where the government may be considering prosecuting the target for criminal violations discovered in the counterintelligence investigation, the government may continue to employ FISA rather than Title III where significant foreign intelligence information is still being sought. Where no significant intelligence interest remains in an investigation, FISA should no longer be used. The determination of whether a significant intelligence interest remains in a given case would continue to be made by the Department of Justice in close consultation with the intelligence agency.

APPENDIX E

UNITED STATES FOREIGN INTELLIGENCE SURVEILLANCE COURT,
WASHINGTON, D.C.

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES FOR AN ORDER AUTHORIZING ELECTRONIC SURVEILLANCES OF

(Docket Number)

MINIMIZATION PROCEDURES

Pursuant to § 101(h) of the Foreign Intelligence Surveillance Act of 1978, the following procedures have been adopted by the Attorney General, and shall be followed by the Federal Bureau of Investigation in implementing these electronic surveillance as ordered by the Court:

Section 1—Applicability and scope

These procedures apply to the acquisition, retention, and dissemination of non-publicly available communications concerning unconsenting United States persons that is collected in the course of electronic surveillance directed at the communications of these agents of a foreign power, consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information. These procedures also apply to non-United States persons only where set forth hereinafter.

Section 2—Definitions

(a) Definitions set forth in § 101 of the Foreign Intelligence Surveillance Act, including the terms "foreign intelligence information," "United States person," and others which may be used in these procedures, shall apply to these procedures.

(b) As used herein "communications of a United States person" includes all communications to which a United States person is a party. "Communications concerning a United States person" includes all communications in which a United States person is discussed or mentioned, except that communications are not "communications concerning a United States person" if they reveal only publicly available information about the person.

(c) When the citizenship status of a party to a communication being surveilled is unknown, and no reasonable basis exists for concluding that the party is not a United States person, it is presumed that such party is a United States person.

Section 3—Acquisition

(a) Interception

The FBI may intercept all communications of or concerning United States persons . . . which are carried over communication lines authorized by Court order.

(b) Verification

At the initiation of electronic surveillances the FBI shall verify that the telephone communication line being intercepted is the telephone line of the target. . . .

(c) Recording

Electronic surveillances of the target . . . may either be monitored contemporaneously; recorded automatically; or conducted by a combination of both means.

(1) In the event that all communications are acquired by automatic recording, the monitor of the automatically acquired tape will employ the same principles of logging, indexing, and using the information as if it had been acquired by a live monitor.

(2) FBI personnel who monitor the electronic surveillances contemporaneously or who monitor automatically acquired information shall exercise reasonable judgment in determining whether particular information intercepted must be minimized.

(3) A permanent written record or "log" shall be maintained by personnel who contemporaneously monitor communications being surveilled or who monitor automatically acquired information; provided that identities or communications of or concerning United States persons that could not be foreign intelligence information or are not evidence of a crime which has been, is being, or is about to be committed may not be logged or summarized.

(e) Non-pertinent Communications

(1) Communications of United States persons acquired in these surveillances will be the subject of continuing analysis:

(a) to establish categories of communications that are not pertinent to the authorized purpose of the survillances;

(b) to eliminate communications in established categories from further acquisiton; and

(c) to include any categories established for elimination of acquisition in any future minimization procedures submitted to the Court.

(2) The Attorney General, or his designee, shall periodically determine that information concerning communications . . . of or concerning United States persons that is retained meets the requirements of these procedures and the Foreign Intelligence Surveillance Act.

Section 4—Internal Use and Retention

(a) Indexing

Logged identities of United States persons and communications of or concerning United States persons may be indexed if such identities or communications reasonably appear to be foreign intel-

ligence information or are evidence of a crime which has been, is being, or is about to be committed, and shall be recorded in the Electronic Surveillance Index pursuant to Title 18, United States Code, § 3504 if it meets established indexing criteria for the index.

(b) Transcription, Duplication and Other Records

Communications . . . of or concerning United States persons may be transcribed or duplicated, and reports made of their contents only for authorized foreign intelligence, foreign counterintelligence, counter-sabotage and international terrorism, or law enforcement purposes.

(c) Foreign Intelligence Information

Intercepted communications . . . of or concerning United States persons which contain foreign intelligence information as defined in § 1 may be used only in foreign counterintelligence investigations or for other authorized foreign intelligence or counter-sabotage or international terrorism purposes. Foreign intelligence information which is also evidence of a crime which has been, is being, or is about to be committed may be used as provided in § 4(d) below.

(d) Evidence of Crime Not Otherwise Foreign Intelligence Information

Intercepted communications . . . of or concerning United States persons, that is acquired incidental to the collection of foreign intelligence information and contains information that is evidence of a crime which has been, is being, or is about to be committed, but which is not otherwise foreign intelligence information, may be retained or used only for the purposes of preventing the crime or enforcing the criminal law.

(e) Controlled Access

Strict controls shall be placed on the storage and retrieval of intercepted communications of or concerning United States persons. Use shall be restricted to those FBI supervisory, investigative, and clerical personnel who have a need to know such information to fulfill foreign intelligence or law enforcement responsibilities.

(f) Destruction of Tapes

Tape recordings and duplicate tapes of communications of or concerning United States persons shall be destroyed within a reasonable period of time following their authorized retention and use as provided above, except that:

(1) tapes containing evidence of a criminal offense will be retained until a decision is rendered by prosecutive authorities. If it is decided to prosecute, tapes will be retained until the end of the prosecution process;

(2) tapes containing communications that reasonably appear to be exculpatory ("Brady") material shall be retained as if they contained evidence of a crime;

(3) tapes containing privileged communications will be retained until ordered to be destroyed by the Department of Justice; and

(4) tapes required to be retained by a rule of law or a judicial order will be retained in accordance with the requirements of that rule or order.

Section 5—Dissemination

(a) General Restrictions

(1) Subject to the requirements of § 5(b) of these procedures non-publicly available information concerning United States persons obtained from the electronic surveillances of the target . . . may not be disseminated without the consent of the United States person involved unless the information is, or reasonably appears to be, foreign intelligence information as defined in § 101(e) (1) and (2) of the Foreign Intelligence Surveillance Act or is evidence of a crime which has been, is being, or is about to be committed.

(2) Non-publicly available information concerning United States persons obtained from electronic surveillances of the target . . . which is foreign intelligence information may be disseminated within the Federal Government and only to officials, agencies, or components with responsibilities directly related to the information proposed to be disseminated, and, upon approval of the Attorney General, may be disseminated to foreign governments; information which is evidence of a crime may be disseminated to Federal, state, local, or foreign officials or agencies with law enforcement responsibility for the crime.

(b) Section 101(e)(1) foreign intelligence information

Non-publicly available information concerning United States persons obtained from the electronic surveillances of the target . . . which is or reasonably appears to be foreign intelligence information as defined in § 101(e)(1) of the Foreign Intelligence Surveillance Act may be disseminated in a manner that identifies United States persons only for authorized foreign intelligence, foreign counterintelligence, counter-sabotage and international terrorism, or law enforcement purposes.

(c) Section 101(e)(2) Foreign Intelligence Information

Non-publicly available information concerning United States persons obtained from the electronic surveillances of the target . . . which is or reasonably appears to be foreign intelligence information as defined in § 101(e)(2) of the Foreign Intelligence Surveillance Act may not be disseminated in a manner that identifies any United States person, except by general characterization, unless such person's identity is necessary to understand the information or assess its importance and may be disseminated only for authorized foreign intelligence, foreign counterintelligence, counter-sabotage and international terrorism, or law enforcement purposes.

(d) Criminal Information

Non-publicly available information concerning United States persons obtained from the electronic surveillances of the target . . . which is evidence of a crime which has been, is being, or is about to be committed but which is not or does not reasonably appear to be foreign intelligence information as defined in § 101(e) of the For-

eign Intelligence Surveillance Act may be disseminated only for law enforcement purposes. Any information acquired from electronic surveillances of the target agents of a foreign power which is disseminated for law enforcement purposes shall be accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

APPENDIX F

UNITED STATES FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES FOR AN ORDER AUTHORIZING ELECTRONIC SURVEILLANCE OF

(Docket Number 80–0)

Classified and Extended by: Deputy Counsel for Intelligence Operations, OIP&R, DOJ.
Reason: Intelligence, Sources and Methods; Foreign Relations.
Review on:

MINIMIZATION PROCEDURES

Pursuant to Section 101(h) of the Foreign Intelligence Surveillance Act of 1978, the following procedures have been adopted by the Attorney General, and shall be followed by the National Security Agency in implementing this electronic surveillance as ordered by the Court:

Sec. 1—Applicability and Scope

These procedures apply to the acquisition, retention and dissemination of information concerning United States persons that is collected in the course of electronic surveillance directed at conducted under the Foreign Intelligence Surveillance Act, Public Law 95–511 ("the Act"). The procedures also apply to the

Sec. 2. Definitions

In addition to the definitions in Section 101 of the Act, the following definitions shall apply to these procedures:

(a) *Acquisition* means the interception by the National Security Agency through electronic means of a communication to which it is not an intended party and the processing of the contents of that communication into an intelligible form intended for human inspection.

(b) *Available publicly* means information that a member of the public could obtain on request, by research in public sources, or that has been obtained by casual observation.

(c) *Consent* is the agreement by a person or organization to permit the National Security Agency to take particular actions that affect the person or organization. To be effective, consent must be given by the person or organization against whom the action will be taken, with sufficient knowledge to understand the action that may be taken and the possible consequences of that action. An agreement by an organization with the National Security Agency to permit collection of information shall be deemed valid consent if

given on behalf of such organization by an official or governing body determined by the General Counsel, National Security Agency to have actual or apparent authority to make such an agreement.

(d) *Identification of a United States person* means the name, unique title, address or other personal identifier of a United States person in the context of activities conducted by others and related to that person. A reference to a product by brand name, or manufacturer's name or the use of a name in a descriptive sense, e.g., "Monroe Doctrine", is not an identification of a United States person.

(e) * * *.

(f) *United States person:* the following guidelines apply in determining whether a person whose status is unknown meets the definition of United States person:

(1) A person known to be currently in the United States will be treated as a United States person unless that person is positively identified as an alien who has not been admitted for permanent residence or unless the nature of the person's communications or other indicia in the contents or circumstances of such communications give rise to a reasonable belief that such person is not a United States person.

(2) A person known to be currently outside the United States, or whose location is not known, will not be treated as a United States person unless such person can be positively identified as such or the nature of the person's communications or other indicia in the contents or circumstances of such communications give rise to a reasonable belief that such person is a United States person.

(3) A person known to be an alien admitted for permanent residence in the United States is assumed to have lost his status as a United States person if the person is not in compliance with the administrative formalities provided by law (8 U.S.C. 1203) that enable such persons to re-enter the United States without regard to the provisions of law that would otherwise restrict an alien's entry into the United States. The failure to follow the statutory procedures provides a reasonable basis to conclude that such alien has abandoned any intention of maintaining his status as a permanent resident alien.

(4) An unincorporated association whose headquarters are located outside the United States may be presumed not to be a United States person unless the Agency has information indicating that a substantial number of its members are citizens of the United States or aliens lawfully admitted for permanent residence.

Sec. 3. Acquisition.

The collection of information by electronic surveillance subject to these procedures shall be accomplished in accordance with the certification of the Attorney General or the court order authorizing such surveillance and will be conducted by technical means, and in a manner designed to minimize to the greatest extent reasonably feasible the acquisition of information which is not relevant to the authorized purpose of the surveillance personnel will monitor the collection of raw data at regular intervals to verify that the surveillance is not avoidably acquiring communications of United

States persons outside the authorized scope of the surveillance or information concerning United States persons not related to the purpose of the surveillance. Personnel will discard inadvertently acquired communications of, or information concerning, United States persons at the earliest practicable point in the processing cycle at which such communication or information can be identified as clearly not relevent to the authorized purpose of the surveillance.

Any such communication or information acquired in the course of an authorized surveillance may be retained and disseminated only in accordance with Sections 4 and 5 of these procedures.

Sec. 4. Retention.

Communications of, or information concerning, United States persons intercepted by the National Security Agency in the course of an electronic surveillance subject to these procedures may be retained in the original form or as transcribed only:

(a) * * *.

(b) if dissemination of such communications without elimination of references to such United States persons would be permitted under Section 5 below.

(c) if it contains information that is evidence of a crime that has been, is being, or is about to be committed and is retained to permit dissemination to the appropriate law enforcement authorities.

Sec. 5. Dissemination

(a) Dissemination of intelligence reports based on communications of, or which contain information concerning, an identified unconsenting United States person may only be made if one of the following criteria is met:

(1) the information is available publicly.

(2) the identity of the United States person is necessary to understand foreign intelligence information or assess its importance, e.g., the identity of a senior official in the Executive Branch.

(3) the communication or information indicates that the United States person may be an agent of a foreign power.

(4) the communication or information which is being disseminated indicates that the United States may be:

(A) a foreign power as defined in Section 101(a) (4) or (6) of the Act;*

(B) residing outside the United States and holding an official position in the government or military forces of a foreign-power such that information about his activities would constitute foreign intelligence;*

(C) a corporation or other entity that is owned or controlled directly or indirectly by a foreign power;* or

(D) acting in collaboration with an intelligence or security service of a foreign power and the United States person has, or has had, access to information or material classified by the United States;

* The identity of a United States person in this context is deemed to meet the statutory standard of "necessary to understand or assess" the importance of foreign intelligence information.

(5) the communication or information indicates that the United States person may be the target of intelligence activities of a foreign power.

(6) the communication or information indicates that the United States person is engaged in the unauthorized disclosure of classified national security information, but only after the agency that originated the information certifies that it is properly classified.

(7) the communication of information indicates that the United States person may be engaging in international terrorist activities.

(8) the interception of the United States person's communication was authorized by a court order issued pursuant to Section 105 of the Act and the communication may relate to the foreign intelligence purpose of the surveillance.

(9) the communication or information is evidence that a crime has been, is being, or is about to be committed provided that dissemination is for law enforcement purposes, e.g., the communication or information indicates a possible threat to the life or physical safety of any person.

(b) A report based on a communication of, or information concerning, an unconsenting United States person that is not publicly available may be disseminated without regard to the limitations in (a) above if the identity of the United States person is deleted and a generic term or symbol is substituted so that the information in the context of the communication cannot reasonably be connected with an identifiable United States person.

(c) Reports based on the communications of, or containing information concerning, an identified unconsenting United States person may only be disseminated to a recipient requiring the identity of such person in the performance of official duties.

(d) Upon recognition that a radio communication to which all parties are in the United States has been unintentionally acquired under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, such comunication shall be destroyed promptly unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.

Sec. 6. Special Minimization for Certifications

Notwithstanding any other provision of these procedures if, in the course of surveillance conducted pursuant to an Attorney General certification issued in accordance with the provisions of Sec. 102(*a*) of the Act, NSA acquires the contents of any communication to which a United States person is a party, the communication shall not be disclosed, disseminated, or used for any purpose or retained for longer than twenty-four hours after recognition unless a court order is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

DISSENTING VIEWS

The Congress should repeal the Foreign Intelligence Surveillance Act (FISA) (50 U.S.C. 1801 et seq.), which requires prior judicial approval for foreign electronic surveillance, and restore the law to its pre-FISA status in which the President, in accordance with his powers and duties under Article II of the Constitution, held exclusive authority for electronic surveillance of foreign powers and their agents within the United States for foreign intelligence purposes. The President must have authority to engage in electronic surveillance in the United States for foreign intelligence purposes with great speed and the utmost secrecy, especially in these times of increased danger from hostile foreign nations and from international terroists. Moreover, judges and judicial procedure are ill-suited to make the determinations needed in electronic surveillance of foreign powers and their agents.

INCREASED THREAT TO SECURITY OF THE UNITED STATES

Events in recent times have demonstrated the great degree to which hostile foreign nations have accelerated their espionage activities in the United States. Soviet bloc agents active in the United States have acquired the secrets of an extremely sophisticated, sensitive and valuable satellite system for intelligence collection and the secrets of United States ballistic missile defense efforts. Soviet bloc espionage agencies have engaged in the United States in successful clandestine efforts to acquire sensitive technology which has important military and intelligence applications. Hostile intelligence services have recruited disloyal United States Intelligence personnel who have provided them with a great deal of damaging information on United States intelligence activities. The Soviet KGB and other Communist bloc intelligence services it controls have engaged in a broad range of espionage activities within the United States. To combat these Soviet bloc activities which threaten the security of the Nation, the United States must improve its counterintelligence capabilities. Only through more aggressive counterintelligence activities can the United States parry the Soviet espionage thrust into the United States. Restoring the President's exclusive authority to conduct electronic surveillance for foreign intelligence purposes by repealing the FISA would be an important contribution to an effective, highly secure counterintelligence effort.

In addition to the increased threat to the security of the United States from the espionage activities of hostile foreign nations, the United States faces a similar increased threat from terrorist activities. Forty percent of the terrorist attacks in the world in 1983 were directed at Americans. In November 1983, a powerful bomb exploded in the U.S. Capitol and, but for the luck of an early ad-

journment, Senators probably would have died. The United States presents inviting targets for terrorists because attacks on Americans guarantee maximum publicity.

UNSUITABILITY OF THE JUDICIAL PROCESS FOR FOREIGN INTELLIGENCE DECISIONS

The Supreme Court made clear the special role of the President in intelligence and foreign policy and has expressed the need to refrain from judicial intrusion into such matters:

> The President, both as Commander-in-Chief and as the Nation's organ for foreign affairs, has available intelligence services whose reports are not and ought not to be published to the world. It would be intolerable that courts, without the relevant information, should review and perhaps nullify actions of the Executive taken on information properly held secret. Nor can courts sit in camera in order to be taken into executive confidences. But even if courts could require full disclosure, the very nature of executive decisions as to foreign policy is political, not judicial. Such decisions are wholly confided by our Constitution to the political departments of the government, Executive and Legislative. They are delicate, complex, and involve large elements of prophecy. They are and should be undertaken only by those directly responsible to the people whose welfare they advance or imperil. They are decisions of a kind for which the Judiciary has neither aptitude, facilities nor responsibility and which has long been held to belong in the domain of the political power not subject to judicial intrusion or inquiry.[1]

The FISA flies in the face of this wisdom. A single judge of the Foreign Intelligence Surveillance Court has the power to deny the President, or his duly authorized representatives, the use of electronic surveillance on agents of foreign powers, such as foreign spies or terrorists, engaged in activities hostile to United States interests. Judges are not suited by training or temperament to make the intelligence evaluations and security decisions involved in foreign intelligence electronic surveillances.

The authority for electronic surveillance for foreign intelligence purposes should rest with the President alone. Presidential primacy with respect to such electronic surveillance would best satisfy the need for speed and strict secrecy in United States counterespionage and counterterrorism operations. Moreover, Presidential primacy in such matters is fully consistent with the Constitution and with the protection of the civil liberties of Americans; indeed, by contributing to the security of the Nation, it protects the ability of present and future generations of Americans to exercise their freedoms.

---

[1] *Chicago & Southern Air Lines, Inc.* v. *Waterman Steamship Corp.*, 333 U.S. 103, 111 (1948) (citations omitted).

THE CONSTITUTION AND FOREIGN INTELLIGENCE ELECTRONIC SURVEILLANCE

Article II of the Constitution vests "the executive power" in the President, makes him Commander-in-Chief of the armed forces, gives him the power to make treaties (with Senate concurrence), and gives him the power to appoint ambassadors (with Senate consent) and receive ambassadors.[2] The Supreme Court has recognized that the constitutional scheme provides for presidential primacy in foreign affairs and assigns him ultimate responsibility to protect national security.[3] As recently as 1981, the Supreme Court stated that "matters intimately related to foreign policy and national security are rarely proper subjects for judicial intervention."[4] Nowhere is the need for exclusive presidential authority greater than in protecting this Nation from international terrorism and from the espionage activities of hostile foreign nations, and such matters fall squarely within the national security and foreign affairs realms with respect to which the Supreme Court has repeatedly stated that no appropriate role for the judiciary exists. The courts of the United States have consistently held that the Constitution does not require the President or his authorized representatives to obtain a judicial warrant or order for the conduct of electronic surveillance of foreign powers and their agents for foreign intelligence purposes.[5] The courts which have considered such foreign intelligence electronic surveillance have held squarely and explicitly that the President may, consistently with the Fourth Amendment, authorize electronic surveillance of foreign powers and their agents within the United States without obtaining a judicial warrant.

In *United States* v. *Humphrey and Truong,* 629 F.2d 908, 913–14 (4th Cir. 1980), the United States Court of Appeals for the Fourth Circuit held that the Executive Branch need not obtain a judicial warrant for foreign intelligence electronic surveillances of agents of foreign powers. The Court stated:

> For several reasons, the needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would, following *Keith* [see note 5], "unduly frustrate" the President in carrying out his foreign affairs responsibilities. First of all, attempts to counter foreign threats to the national security require the utmost stealth,

[2] U.S. Const., art. II, sec. 1 (executive power), sec. 2 (Commander-in-Chief) (treaty power) (ambassadorial appointment), and sec. 3 (ambassadorial receipt).

[3] *United States* v. *Curtiss-Wright Export Corp.,* 299 U.S. 304 (1936); *see Chicago & Southern Airlines, supra n. 1.*

[4] *Haig* v. *Agee,* 453 U.S. 280, 292 (1981); see *Harisiades* v. *Shaughnessy,* 342 U.S. 580 (1952) (matters "relating to the conduct of foreign relations . . . are so exclusively entrusted to the political branches of government as to be largely immune from judicial inquiry or interference.")

[5] The holding of the case of *United States* v. *United States District Court,* 407 U.S. 297 (1972), is not to the contrary. The case, known commonly as the *Keith* case after the name of the U.S. district judge involved in the case, stands for the proposition that the Fourth Amendment generally requires a warrant for *domestic security* electronic surveillances within the United States. The Court specifically stated that it did not answer the question whether a warrant is or is not required for a foreign intelligence electronic surveillance in the United States, which involves activities of an agent of a foreign power. Id. 321–22. Similarly, *Zweibon* v. *Mitchell,* 516 F.2d 594 (D.C. Cir. 1975), *cert. denied* 425 U.S. 944 (1976), did not deal with a foreign intelligence surveillance of an agent of a foreign power.

speed, and secrecy. A warrant requirement would add a procedural hurdle that would reduce the flexibility of executive foreign intelligence initiatives, in some cases delay executive response to foreign intelligence threats, and increase the chance of leaks regarding sensitive executive operations.

More importantly, the executive possesses unparalleled expertise to make the decision whether to conduct foreign intelligence surveillance, whereas the judiciary is largely inexperienced in making the delicate and complex decisions that lie behind foreign intelligence surveillance.

The executive branch, containing the State Department, the intelligence agencies, and the military, is constantly aware of the nation's security needs and the magnitude of external threats posed by a panoply of foreign nations and organizations. On the other hand, while the courts possess expertise in making the probable cause determination involved in surveillance of suspected criminals, the courts are unschooled in diplomacy and military affairs, a mastery of which would be essential to passing upon an executive branch request that a foreign intelligence wiretap be authorized. Few, if any, district courts would be truly competent to judge the importance of particular information to the security of the United States or the "probable cause" to demonstrate the government in fact needs to recover that information from one particular source.

Perhaps most crucially, the executive branch not only has superior expertise in the areas of foreign intelligence, it is also constitutionally designated as the pre-eminent authority in foreign affairs.

The President and his deputies are charged by the constitution with the conduct of the foreign policy of the United States in times of war and peace. Just as the separation of powers in *Keith* forces the executive to recognize a judicial role when the President conducts domestic security surveillance, so the separation of powers requires us to acknowledge the principal responsibility of the President for foreign affairs and concomitantly for foreign intelligence surveillance.

In sum, because of the need of the executive branch for flexibility, its practical experience, and its constitutional competence, the courts should not require the executive to secure a warrant each time it conducts foreign intelligence surveillance. [Citations omitted.]

Similarly, in *United States* v. *Brown,* 484 F.2d 418, 426 (5th Cir. 1973), *cert. denied,* 415 U.S. 960 (1974), the U.S. Court of Appeals for the Fifth Circuit stated:

> . . . [B]ecause of the President's constitutional duty to act for the United States in the field of foreign relations, and his inherent power to protect national security in the context of foreign affairs, we reaffirm . . . that the President may constitutionally authorize warrantless wiretaps

for the purpose of gathering foreign intelligence. [Citations omitted.]

The decisions of the U.S. Courts of Appeals for the Third Circuit in *United States* v. *Butenko,* 494 F.2d 593 (3rd Cir. 1974) (en banc), *cert. denied sub nom. Ivanov* v. *United States,* 419 U.S. 881 (1974), and for the Ninth Circuit in *United States* v. *Buck,* 548 F.2d 871 (9th Cir. 1977), *cert. denied* 434 U.S. 890 (1977), are in agreement with the *Humphrey and Truong* and *Brown* decisions quoted above.

In these cases, the United States Courts of Appeals for the Third, Fourth, Fifth, and Ninth Circuits have all concluded that Article II of the Constitution authorizes the President of the United States to engage in foreign intelligence electronic surveillances of foreign powers and agents of foreign powers within the United States, and that the Fourth Amendment does not require the President to obtain a judicial warrant for such surveillances. It is thus eminently clear in the law that the Constitution does not mandate the Foreign Intelligence Surveillance Act, or any similar legislation by which the President would be required to obtain the approval of a court to surveil a foreign power or an agent of a foreign power within the United States.

CONCLUSION

Although the courts have repeatedly made clear that the Constitution authorizes the President to undertake foreign intelligence electronic surveillance consistent with the Fourth Amendment without prior judicial approval, the Congress commanded judicial activism in foreign intelligence electronic surveillance when it adopted the Foreign Intelligence Surveillance Act of 1978. In the FISA, the Congress mandated that the Executive Branch obtain the approval of a judge to engage in foreign intelligence electronic surveillance within the United States of foreign powers and their agents. The Congress required such prior judicial approval despite judges' lack of training in intelligence, diplomatic and military matters; despite the unsuitability of the judicial process for making delicate national security judgments; and despite the great need for speed and absolute secrecy in foreign intelligence electronic surveillance.

The Constitution places upon the President of the United States the duty to protect this Nation from threats from abroad. The United States currently faces an acute threat to its national security from espionage by hostile foreign nations and from the violence of international terrorists. To counter these growing threats to the security of the Nation, the President should be able, consistently with the Constitution, to bring effectively to bear against agents of hostile foreign powers the full counterintelligence and counterterrorism capabilities of the federal government. Foreign intelligence electronic surveillance of these agents of foreign powers is a critical element of these capabilities.

The Congress should, therefore, repeal the Foreign Intelligence Surveillance Act, restoring to the President the full power the Constitution grants him to authorize, without a judge's prior approval, electronic surveillance within the United States of foreign powers and their agents for foreign intelligence purposes. Repeal of the

FISA would assist greatly in the preservation, protection and defense of the Nation against externally-generated dangers.

C. W. BILL YOUNG.
BOB STUMP.

O